ABSTRACT

A method and apparatus are disclosed for simultaneously establishing a user's identity and membership in multiple groups, using only a single identification card (or computer file). In a registration or enrollment phase, secret information is created between the user and any groups for which the user has registered. Once the user has been registered with one or more groups, the user may be authenticated to a verification agent to obtain access to one or more selected groups by providing an encrypted authentication request based on public identifiers relating to one or more groups, and an exponential function based on private identifiers and several randomly generated numbers. The verification agent is able to verify the user's registration with the selected groups without knowing the secret information. Optionally, for additional reliability, the verification agent may request the user to repeat the authentication process multiple times, each time altering one of the random numbers. Once verification is complete, the verification agent arranges for the user to access the selected groups. Significantly, the user is able to authenticate itself with multiple groups by carrying out a single authentication sequence.